Guía de Seguridad Digital para Feministas Autogestivas

Adaptado a partir del trabajo de Noah Kelley (autor) y de Inti (traductora), del colectivo HACK*BLOSSOM.

Guía completa en: https://es.hackblossom.org/cybersecurity/

Anonimato



¿Qué tan invisibles somos en Internet?

- Si no cifrás tu actividad en Internet, NO es privada y es probable que alguien (o algo) la pueda ver.
- Dejadas al azar, las “cookies” brindaran datos personales a las empresas privadas.
- La wifi pública es tan, tan insegura.

Privacidad y Seguridad Sin Esfuerzo: Extensiones de Navegador

- Privacy Badger
- Adblock Plus
- Disconnect.me
- HTTPS Everywhere! (HTTPS en todos lados)

Navegar Anónima: Tor

- Si estás en una situación adonde NECESITÁS ser anónima, por razones de seguridad o actividad política, debés usar la Red Tor.
- Tor te hace anónima, pero NO es privado cuando visitas sitios o servicios que se pueden asociar con tu identidad.

Mejor seguridad con algún esfuerzo + y costo potencial: VPN

- Virtual Private Network.
- Crea una conexión privada, cifrada, entre tu computadora y un servidor de VPN.
- Proveedores de VPN:
  - Pagos: CyberGhost - Private Internet Access.
  - Gratuitos: TunnelBear - Windsricbe

Anonimato y Amnesia Definitiva: Tails

- Tails es un sistema operativo portátil basado en Linux y diseñado específicamente para la privacidad personal.
- Totalmente amnésico: no guarda ningún dato entre cada sesión.
- Lo podés llevar en un DVD o un USB, y usarlo para iniciar desde casi cualquier computadora sin tener que instalar nada.

Protegé tus cuentas digitales.



Ingeniería Social y Phishing (pesca de datos)

- No entres a sitios web desde un link en un email.
- Evitá usar Facebook, Twitter o Google para acceder a otros sitios.
- No confíes en e-mails que piden tu información privada.
- Usá conexiones con HTTPS en lo posible.
- Cuidado con la wi-fi pública.
- En general: entregar información **solo si es crucial**.

Buenas Contraseñas

- Mezcla aleatoria de letras, números y caracteres especiales.
- Cuanto más largas, mejores.
- Si vas a usar palabras reales en tu contraseña, que sean poco conocidas o mal escritas.
- **Tip**: usar acrónimos y otras **fórmulas nemotécnicas** para generar contraseñas difíciles de adivinar pero fáciles de recordar.
- NO REPITAS LA MISMA CONTRASEÑA EN MÚLTIPLES SITIOS.

Administradores de claves

- Aplicaciones que te permiten manejar todas tus contraseñas con una única contraseña maestra (esto también tiene sus riesgos).
- Generador de contraseñas robustas.
- **No usar para contraseñas críticas**, como la del e-mail o el banco.
- Recomendados:
  - KeePassXC (almacenamiento offline)
  - Lastpass (almacenamiento online)

Autenticación Doble (2FA)

- Antes de entrar, necesitás no solo una contraseña sino también un dato más.
- Es generalmente un código enviado por email, SMS o generado por una aplicación celular.
- Los servicios online más usados ya tienen esta opción.
- Authy: aplicación que genera códigos fuera de linea, donde sea que la tengas instalada.

Tus archivos, fotos, videos, son tuyos.



¿Qué pasa si...

- ...alguien se roba tu computadora portátil?
- ...cuando hackean al servicio en la nube que utilizás?
- ...si esa aplicación que te bajaste tan útil, tiene vulnerabilidades que filtran tus datos a hackers?
- **Sí tenés archivos, fotos, o videos que no están cifrados**, **NO son privados**, y deberías asumir que alguien los puede ver.

¿Qué es el cifrado?

- Es un proceso que transforma tus datos en basura ilegible que nadie puede entender lo que significa, excepto las persona que vos elijas.
- PGP (Pretty Good Privacy): funciona con una llave de cifrado que tiene una parte pública y otra privada.
- ¿Qué cifrar?
  - Disco duro.
  - Teléfono.
  - Comunicaciones.
  - Archivos en la nube.

Los celulares nunca serán seguros pero vale la pena intentarlo.

¿A quién le confiás tu teléfono?

- Fabricantes
- Sistema operativo
- Aplicaciones
- Proveedor de telecomunicaciones
- ¿Y si si es extraviado, robado o hackeado?

Protegé tu teléfono con cifrado

- Se configura en los ajustes de seguridad en el propio teléfono.
- Requiere PIN o contraseña (no funciona con huella, reconocimiento facial o de voz).
- Nadie podrá acceder a tus datos personales (fotos, vídeos, cuentas bancarias, etc.) si no conoce la clave.
- No impide la minería de datos, el rastreo de localización, ni el monitoreo.

Protegé tus mensajes de texto y llamadas

- Usá Signal: aplicación de código abierto, que habilita enviar y recibir llamadas y mensajes cifrados.
- La única información que se transmite es: quien llamó o mandó el mensaje, quien lo recibió y cuando se recibió. Terceros no pueden acceder el contenido.
- Los mensajes de texto a quienes no usan Signal no serán cifrados.
- Si las dos personas se comunican por Internet, la comunicación es gratis ¡y sin esfuerzo!

Protegé tu navegación

- Usar los servicios de Tor en distintas aplicaciones del teléfono con Orbot.
- Navegar con Orfox.
- OpenVPN como cliente VPN (Android).

No permitas que los trolls espíen tus pensamientos y experiencias privadas.

¿Qué hacen las plataformas online con nuestros datos?

- Es casi imposible garantizar un nivel real de privacidad mientras dependemos de empresas privadas para poder comunicarnos.

- Como estas empresas privadas guardan tus datos indefinidamente, tus conversaciones de hoy y ayer serán accesibles por muchos años en el futuro.

Seguridad en los Medios Sociales

- Atenta al pihshing y métodos de ingeniería social.
- Autenticación doble y contraseñas seguras.
- Cuidado con usar GPS (Geotagging).
- No confíes en aplicaciones que requieren acceso a tus cuentas.
- Familiarizate con las opciones de privacidad.

Chats seguros: OTR

- OTR (Off The Record): protocolo para cifrar mensajería entre vos y el receptor.
- Se puede utilizar con una gran variedad de servicios de mensajería (Google Hangouts, Facebook Messenger, etc.)
- Lo único que necesitás en un clinte de chat con OTR habilitado: Pidgin, CoyIM, Jitsi (para la compu), Conversations (Android), Chatsecure (iOS).

Chats sin control corporativo con XMPP

- Servicio descentralizado y de codigo-abierto.
- Es como el "correo electrónico" de la mensajería instantánea: podés hablar con cualquier persona aunque no tenga su cuenta en el mismo servicio.
- Hay que crear una cuenta, por ejemplo en https://mijabber.es/ o en https://www.suchat.org (hay cientos de opciones y todos los servicios se comunican entre sí).
- Elegir un cliente de chat como los mencionados antes.

Protegé tus conversaciones en email con cifrado

- Necesitás:
  - Una llave privada para “firmar”.
  - Dar a conocer tu llave pública, por ejemplo en tu firma de correo.
  - Tener las llaves públicas de tus contactos.



Protegé tus conversaciones en email con cifrado

- Se puede usar:
  - En los servicios de webmail más conocidos (Gmail, Yahoo, Outlook, etc.) utilizando la extensión Mailvelope en Firefox o Chrome.
  - Configurando opciones de seguridad en tu cliente de correo (Thunderbird, Outlook, Apple Mail y otros).
  - Usar un servicio de correo que integre un protocolo de cifrado. Por ejemplo: Disroot, Protonmail, Openmailbox.

Las mejores herramientas para tus necesidades de seguridad digital.

Uso Casual de Internet

- Instalar extensiones de privacidad en el navegador.
- Autenticación doble para tus cuentas digitales.
- Contraseñas muy fuertes y únicas y/o gestor de contraseñas.
- Bajar Tor para navegar anónima cuando sea necesario.
- Encriptar tu teléfono celular y tu computadora.

Conversaciones Privadas

- Encriptar mensajes de texto en tu teléfono inteligente.
- Encriptar mensajería instantánea con OTR.
- Enviar e-mails encriptados.
- Hacer llamadas encriptadas con tu teléfono inteligente.
- Encriptar tu teléfono y computadora.

Anonimato Avanzado

- Escondé tu locación física y encriptá tu conexión con VPN en tu computadora y tu celular.
- Navega anónimamente con Tor.
- Usá una dirección falsa de e-mail para crear cuentas digitales.